Unbounded-Error Classical and Quantum Communication Complexity

Kazuo Iwama[1*] Harumichi Nishimura[2†] Rudy Raymond[3] Shigeru Yamashita[4‡]
[1]School of Informatics, Kyoto University, iwama@kuis.kyoto-u.ac.jp
[2]School of Science, Osaka Prefecture University, hnishimura@mi.s.osakafu-u.ac.jp
[3]Tokyo Research Laboratory, IBM Research, raymond@jp.ibm.com
[4]Nara Institute of Science and Technology, ger@is.naist.jp

Abstract

Since the seminal work of Paturi and Simon [26, FOCS'84 & JCSS'86], the unbounded-error classical communication complexity of a Boolean function has been studied based on the arrangement of points and hyperplanes. Recently, [14, ICALP'07] found that the unbounded-error *quantum* communication complexity in the *one-way communication* model can also be investigated using the arrangement, and showed that it is exactly (without a difference of even one qubit) half of the classical one-way communication complexity. In this paper, we extend the arrangement argument to the *two-way* and *simultaneous message passing* (SMP) models. As a result, we show similarly tight bounds of the unbounded-error two-way/one-way/SMP quantum/classical communication complexities for *any* partial/total Boolean function, implying that all of them are equivalent up to a multiplicative constant of four. Moreover, the arrangement argument is also used to show that the gap between *weakly* unbounded-error quantum and classical communication complexities is at most a factor of three.

1 Introduction

As with many other probabilistic computation models, *communication complexity* (CC for short) has two contradistinctive settings: *Bounded-error* CC refers to the amount of communication (the number of bits exchanged) between Alice and Bob which is enough to compute a Boolean value $f(x, y)$, with high probability, from Alice's input x and Bob's input y. On the other hand, *unbounded-error* CC refers to the lowest possible amount of communication which is needed to give "a positive hint" for the computation of $f(x, y)$, in other words, even one-bit less communication would be the same as completely no communication in the worst case. More formally, it is defined as the minimum amount of communication between Alice and Bob such that for all x and y Alice (or Bob) can output a correct value of $f(x, y)$ with probability $> 1/2$.

Unbounded-error CC was first studied by Paturi and Simon [26], who characterized its one-way version, $C^1(f)$, in terms of the minimum dimension k_f of the *arrangement* that realizes the Boolean function f (see Sec. 2 for the definition of arrangements). Namely they showed $\lceil \log k_f \rceil \leq C^1(f) \leq \lceil \log(k_f + 2) \rceil$. It was also proven that the two-way (unbounded-error) CC, $C(f)$, does not differ from $C^1(f)$ more than one bit for any (partial or total) Boolean function f, which is a bit surprising since there are easily seen exponential differences between them in the bounded-error setting (see, say [21]).

Since then, arrangement has been a standard tool for studying unbounded-error CC. Alon, Frankl, and Rödl [1] showed by counting arguments that almost all Boolean functions have linear unbounded-error CCs. The first linear lower bound of an explicit function was found by Forster [8],

*Supported in part by Scientific Research Grant, Ministry of Japan, 16092101 and 19200001.
†Supported in part by Scientific Research Grant, Ministry of Japan, 19700011.
‡Supported in part by Scientific Research Grant, Ministry of Japan, 16092218 and 19700010.

who gave the linear lower bound of the inner product function by showing the lower bound of its minimum dimension using operator norms. Extending Forster's arguments, there are several papers on the study of unbounded-error CC [9, 10] that also put emphasis on the margin of arrangements.

Recently, [14] completely characterized the unbounded-error one-way (Alice to Bob) quantum CC, $Q^1(f)$, also in terms of k_f, i.e., $Q^1(f) = \lceil \log \sqrt{k_f + 1} \rceil$. The main idea was to relate quantum states in Alice's side and POVMs in Bob's side to points and hyperplanes of a real space arrangement, respectively. Moreover, they also closed the small gap between the upper and lower bounds of $C^1(f)$ in [26] by proving $C^1(f) = \lceil \log(k_f + 1) \rceil$. As a result, they found that the unbounded-error one-way quantum CC of any Boolean function is always exactly one half of its classical counterpart. Unfortunately, however, their studies were limited within the one-way model: The proof technique mentioned above apparently depends on the one-way communication and there is no obvious way of its extension to the more general two-way communication model. Furthermore, it seems hard to change two-way *quantum* protocols to one-way quantum protocols efficiently, which was possible and was used as the basic approach in the classical case [26].

Our Contribution. We provide a new approach for constructing an arrangement from a given two-way quantum protocol with n qubit communication. The basic idea is to use the simple fact, found by Yao [30] and Kremer [20], that the final state of the whole system after the protocol is finished can be written as a superposition of at most 2^n different states. This allows us to imply a quite tight lower bound for the two-way quantum CC $Q(f)$, namely $Q(f) \geq \lceil \log \sqrt{k_f + 1/8} - 1/2 \rceil$. Notice that this lower bound does not differ more than one qubit from the upper bound of one-way CC $Q^1(f)$ in [14], which then means that all of $Q(f)$, $Q^1(f)$, $C(f)/2$ and $C^1(f)/2$ coincide within the difference of at most only one bit or one qubit.

Arrangements are also useful to provide a couple of related results: First, we give almost tight characterizations of $Q^{||}(f)$ and $C^{||}(f)$, i.e., the unbounded-error quantum and classical CCs in the *simultaneous message passing* (SMP) model. We prove that $Q^{||}(f)$ and $C^{||}(f)$ are equal to twice as much as $Q^1(f)$ and $C^1(f)$ up to a few qubits and bits, respectively. Therefore we can see that in the unbounded-error setting all of the two-way/one-way/SMP quantum/classical CCs of any Boolean function are asymptotically equivalent up to a multiplicative constant of four. Note that, in the bounded-error classical case, the equality function gives an exponential gap between one-way and SMP CCs [4, 24]. In the bounded-error quantum case, it is also shown that an exponential gap between one-way and SMP CCs exists for some *relations* [12].

Secondly, we give several relations among CCs in the *weakly unbounded-error* setting, which was introduced by Babai et al. [3]. The weakly unbounded-error (classical) CC of a protocol P, denoted by $C_w(P)$, is measured by the sum of the communication cost of P and $\log 1/(p - 1/2)$ if P's success probability is p. The weakly unbounded-error CC of f, $C_w(f)$, is the minimum of $C_w(P)$ over all protocols P that computes f. The quantum variant and one-way/SMP variants are defined similarly. Using two quantities of arrangement, margin and dimension, we show several upper bounds of weakly unbounded-error CCs, in particular, $C_w(f) \leq 3Q_w(f) + O(1)$. Previously, it is only known [17] that $C_w(f) = O(Q_w(f))$. The multiplicative factor three seems to be quite tight since at least a factor of two must be involved as a gap between quantum and classical communication costs as mentioned before.

Related Work. In the bounded-error setting, CCs of some Boolean functions have large gaps between quantum and classical cases: Exponential separations are known for all of two-way [27], one-way [11] and SMP models [5], where the first two cases are for partial Boolean functions, and the last case is for a total Boolean function. It remains to show (if any) exponential gaps for total Boolean functions in the cases of two-way and one-way models. In particular, the largest known gap between quantum and classical one-way CCs is only a factor of two.

Other than the minimum dimension k_f of arrangements, several different measures of Boolean

functions also appeared in the literature. Paturi and Simon [26] showed that $C^1(f)$ (and $C(f)$) is equal to the logarithm of the *sign-rank*, $srank(f)$, up to a few bits (also see [6]). Due to Klauck [17], both $C_w(f)$ and $Q_w(f)$ are equivalent to the logarithm of the inverse of the *discrepancy* $disc(f)$ (see, say [21]) within a constant multiplicative factor and a logarithmic additive factor. The recent result by Linial and Shraibman [22, 23] implies that the maximal margin of arrangements realizing f, $m(f)$, is equivalent to $disc(f)$ up to a multiplicative constant. Thus, combined with the results of the current paper, (i) $C(f)$, $Q(f)$, $\log k_f$ and $\log srank(f)$ are all within a factor of two, and (ii) $C_w(f)$, $Q_w(f)$, $\log disc^{-1}(f)$ and $\log m^{-1}(f)$ within a factor of some constant and a logarithmic additive term. However, due to the two independent results by Buhrman et al. [6] and Sherstov [28], (i) is exponentially smaller than (ii) for some Boolean function f.

2 Technical Components

In this section, we present some basic tools for obtaining our results. Their proofs, as well as some of those in the following sections, are omitted due to space constraints. They are mainly the concept of arrangement and its sufficient conditions (Lemmas 2.3 and 2.4) for realizing a quantum protocol whose success probability can be calculated from arrangement parameters by Lemma 5 in [14].

Arrangements. We denote a point in $\mathbb{R}^n$ by the corresponding n-dimensional real vector, and a hyperplane $\{(a_i) \in \mathbb{R}^n \mid \sum_{i=1}^n a_i h_i = h_{n+1}\}$ by the $(n+1)$-dimensional real vector $\mathbf{h} = (h_1, \ldots, h_n, h_{n+1})$, meaning that any point (a_i) on the plane satisfies the equation $\sum_{i=1}^n a_i h_i = h_{n+1}$. A Boolean function f on $X \times Y$ is *realizable by an arrangement* of a set of $|X|$ points $\mathbf{p}_x = (p_1^x, \ldots, p_k^x)$ and a set of $|Y|$ hyperplanes $\mathbf{h}_y = (h_1^y, \ldots, h_k^y, h_{k+1}^y)$ in $\mathbb{R}^k$ if for any $x \in X$ and $y \in Y$, $\mathrm{sign}(\sum_{i=1}^k p_i^x h_i^y - h_{k+1}^y) = f(x,y)$. Here, $\mathrm{sign}(a) = 1$ if $a > 0$ and -1 if $a < 0$. The value $\left|\sum_{i=1}^k p_i^x h_i^y - h_{k+1}^y\right|$ denotes how far the point $\mathbf{p}_x$ lies from the plane $\mathbf{h}_y$, and the *margin* of an arrangement denotes the smallest of such values in the arrangement. The *magnitude* of the arrangement is defined as $\max_{x,y}\left(\sqrt{\sum_{i=1}^k |p_i^x|^2}, \sqrt{\sum_{i=1}^k |h_i^y|^2}, |h_{k+1}^y|\right)$. The value k is called the *dimension* of the arrangement. Let k_f denote the minimum dimension of all arrangements that realize f.

Remark. In the hereafter, our statements will use "functions" while their proofs, that obviously hold for partial, are showed only for total ones. Note also that the concept of arrangement in this paper is not *symmetric*. Here, Alice's input x and Bob's input y are associated with a point and a hyperplane, respectively. For this reason, the value of k_f might be different from that of k_{f^t}, where $f^t(x,y) := f(y,x)$. However, it can be easily seen that $|k_f - k_{f^t}| \leq 1$. The random access coding is one of examples such that $|k_f - k_{f^t}| = 1$ [2, 14].

The following lemma relates arrangements to classical CC, which was shown in [26] and later in [9] in more detail including the margin.

Lemma 2.1 (From arrangements to classical CC) *Any N-dimensional arrangement realizing f of magnitude at most 1 with margin μ can be converted into a classical one-way protocol for f using at most $\lceil \log(N+1) \rceil + 1$ bits with success probability at least $1/2 + \mu/(2\sqrt{N+1})$.*

Bloch Vector Representations of Quantum States. Let $N = 2^n$. Any n-qubit state can be represented by an $N \times N$ positive matrix $\boldsymbol{\rho}$ (also often called N-level quantum state), satisfying $\mathrm{Tr}(\boldsymbol{\rho}) = 1$. Moreover, $\boldsymbol{\rho}$ can be written as a linear combination of N^2 *generator matrices* $\boldsymbol{I}_N, \boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{N^2-1}$, where $\boldsymbol{I}_N$ is the identity matrix (the subscript N is often omitted when it is clear from the context), and $\boldsymbol{\lambda}_i$'s are $N \times N$ matrices which are generators of $SU(N)$ satisfying (i)

$\boldsymbol{\lambda}_i = \boldsymbol{\lambda}_i^\dagger$ (i.e., $\boldsymbol{\lambda}_i$'s are Hermitian), (ii) $\mathrm{Tr}(\boldsymbol{\lambda}_i) = 0$ and (iii) $\mathrm{Tr}(\boldsymbol{\lambda}_i\boldsymbol{\lambda}_j) = 2\delta_{ij}$. Note that $\boldsymbol{\lambda}_i$ can be any generator matrices satisfying the above conditions (and in fact N can be any positive integer ≥ 2), but practically for $n = 1$ one can choose $\boldsymbol{\sigma}_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $\boldsymbol{\sigma}_3 = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}$ of Pauli matrices as $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2$, and $\boldsymbol{\lambda}_3$, respectively. For larger n, one can choose the following tensor products of Pauli matrices for $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{N^2-1}$: $\boldsymbol{\lambda}_1 = \sqrt{\frac{2}{N}}\boldsymbol{I}_2^{\otimes n-1} \otimes \boldsymbol{\sigma}_1$, $\boldsymbol{\lambda}_2 = \sqrt{\frac{2}{N}}\boldsymbol{I}_2^{\otimes n-1} \otimes \boldsymbol{\sigma}_2$, $\boldsymbol{\lambda}_3 = \sqrt{\frac{2}{N}}\boldsymbol{I}_2^{\otimes n-1} \otimes \boldsymbol{\sigma}_3$, $\boldsymbol{\lambda}_4 = \sqrt{\frac{2}{N}}\boldsymbol{I}_2^{\otimes n-2} \otimes \boldsymbol{\sigma}_1 \otimes \boldsymbol{I}, \ldots, \boldsymbol{\lambda}_{N^2-2} = \sqrt{\frac{2}{N}}\boldsymbol{\sigma}_3^{\otimes n-1} \otimes \boldsymbol{\sigma}_2$, and $\boldsymbol{\lambda}_{N^2-1} = \sqrt{\frac{2}{N}}\boldsymbol{\sigma}_3^{\otimes n}$. The following representation is known on N-level quantum states (see, e.g., [16]).

Lemma 2.2 *For any N-level quantum state $\boldsymbol{\rho}$ and any $N \times N$ generator matrices $\boldsymbol{\lambda}_i$'s, there exists an (N^2-1)-dimensional vector $\mathbf{r} = (r_i)$ such that $\boldsymbol{\rho}$ can be written as*

$$\boldsymbol{\rho} = \frac{1}{N}\left(\boldsymbol{I} + \sqrt{\frac{N(N-1)}{2}}\sum_{i=1}^{N^2-1} r_i\boldsymbol{\lambda}_i\right).$$

The vector $\mathbf{r}$ in this lemma is often called the *Bloch vector* of $\boldsymbol{\rho}$.

Note that Lemma 2.2 is a necessary condition for $\boldsymbol{\rho}$ to be a quantum state. The following sufficient condition appeared in [14], using the geometric fact of Bloch vectors in [15, 19].

Lemma 2.3 *For any $\mathbf{r} = (r_1, r_2, \ldots, r_k) \in \mathbb{R}^k$ and any N satisfying $N^2 \geq k+1$,*

$$\boldsymbol{\rho}(\mathbf{r}) = \frac{1}{N}\left(\boldsymbol{I} + \sqrt{\frac{N(N-1)}{2}}\sum_{i=1}^{k}\left(\frac{r_i}{|\mathbf{r}|(N-1)}\right)\boldsymbol{\lambda}_i\right)$$

is an N-level quantum state. (Intuitively, if a vector is shrunk enough to be inside the ball of radius $1/(N-1)$, its shrunk vector is always a quantum state.) Moreover, if $\boldsymbol{\rho}(\mathbf{r})$ is a quantum state, then $\boldsymbol{\rho}(\gamma\mathbf{r})$ is also a quantum state for any $0 \leq \gamma \leq 1$.

Bloch Vector Representations of POVMs. A POVM $M = \{\boldsymbol{E}, \boldsymbol{I}-\boldsymbol{E}\}$ is a set of operators, which represents a quantum measurement, such that $\boldsymbol{E}$ and $\boldsymbol{I}-\boldsymbol{E}$ are positive matrices. It is known that any POVM M on N-level quantum states can be written as a linear combination of $N \times N$ generator matrices $\boldsymbol{\lambda}_i$'s. Namely,

$$\boldsymbol{E} = e_{N^2}\boldsymbol{I} + \sum_{i=1}^{N^2-1} e_i\boldsymbol{\lambda}_i,$$

where $\mathbf{e} = (e_1, e_2, \ldots, e_{N^2})$ is called the *Bloch vector representation* of POVM M. One sufficient condition for a vector to represent a POVM is given as follows.

Lemma 2.4 *Let $\mathbf{e} = (e_1, e_2, \ldots, e_{N^2}) \in \mathbb{R}^{N^2}$ such that*

$$\sum_{i=1}^{N^2-1} e_i^2 \leq \frac{N}{2(N-1)}\min(e_{N^2}^2, (1-e_{N^2})^2).$$

If we take $\boldsymbol{E} = e_{N^2}\boldsymbol{I} + \sum_{i=1}^{N^2-1} e_i\boldsymbol{\lambda}_i$, then $\{\boldsymbol{E}, \boldsymbol{I}-\boldsymbol{E}\}$ is a POVM on N-level quantum states.

3 Two-Way Communication Complexity

The model is due to Yao [30]: The space of a quantum protocol consists of Alice and Bob's private parts and a communication channel. On her (his) turn, Alice (Bob) applies a unitary transformation

on her (his) part and the communication channel, and Bob (Alice) receives quantum information from the content of the channel. Finally the output of the protocol is obtained by a measurement via Alice or Bob. Note that without loss of generality we can assume that no measurement is performed in the middle of the protocol. This is because it is well known that measurements can be postponed without increasing the communication cost [25]. Also, it is often assumed, for technical reason, that the output is put on the communication channel. A protocol described under this output style (and Yao's formalism), which we call a *shared-output* protocol, means that the protocol's output can be known to *both* Alice and Bob. We define $Q(f)$ as the CC for *one of them* to know the output since we want to regard one-way protocols as a special case of two-way protocols. Thus our $Q(f)$ may be smaller than the corresponding CC under shared-output protocols, but we can easily see that the gap is at most one qubit.

For the shared-output protocol, the following lemma, which was given by Yao [30] without proof and proved by Kremer [20], is quite strong.

Lemma 3.1 ([30] and [20]) *The final state of a shared-output quantum protocol for a Boolean function f on input (x, y) using n qubit of communication can be written as*

$$\sum_{i\in\{0,1\}^n} |A_i(x)\rangle|i_n\rangle|B_i(y)\rangle,$$

where $|A_i(x)\rangle$ and $|B_i(y)\rangle$ are complex vectors of norm ≤ 1, and i_n is the nth bit of the index i and also the last bit of the communication channel (that is, the output bit).

To see the intuitive meaning of this lemma might help understand the proof of Lemma 3.3 (our main lemma) more easily. There are two points: (i) The superposition consists of at most 2^n different states, independent of the size of the whole space. This allows us to consider only 2^{2n} ($2^n \times 2^n$) different combinations of vectors (and their inner product values) when calculating the trace of underlying density matrices whose size may be much larger. (ii) As one can see, a product of state $A_i(x)$ and state $B_j(y)$ exists only if $i = j$. This correspondence is translated into the same correspondence between the indices when calculating an inner product of a point and a hyperplane of the converted arrangement. A similar correspondence was also used in [7] for lower bounds of quantum exact and bounded-error protocols, and in [29] for tight lower bounds of quantum one-sided unbounded-error (which is referred as *nondeterministic*) protocols.

Let $k_f^* = \min(k_f, k_{f^t})$. Then here is our first main result.

Theorem 3.2 *For any Boolean function f, $\lceil \log \sqrt{k_f + 1/8} - 1/2 \rceil \leq Q(f) \leq \lceil \log \sqrt{k_f^* + 1} \rceil$.*

Theorem 3.2 induces the equality of two-way and one-way quantum CCs of a Boolean function within one qubit since we can verify that the difference of the upper bound from the lower bound is at most one for any integer $k_f > 0$. Recall that the difference between the two-way and one-way CCs is also at most one in the classical case [26]. For the proof of Theorem 3.2, it is enough to give the lower bound $Q(f) \geq \lceil \log \sqrt{k_f + 1/8} - 1/2 \rceil$ since $Q(f) \leq \min(Q^1(f), Q^1(f^t)) = \lceil \log \sqrt{k_f^* + 1} \rceil$. To do so, we relate quantum communication protocols to arrangements.

Lemma 3.3 (From quantum CC to arrangements) *An n-qubit shared-output protocol that computes a Boolean function f with success probability $1/2+\epsilon$ can be converted to a $(2^{2n-1}-2^{n-1})$-dimensional arrangement of magnitude at most 1 that realizes f with margin ϵ.*

Proof. Suppose that P is an n-qubit protocol for f. According to Lemma 3.1, we can write the

final quantum state of P on input (x,y), $\boldsymbol{\rho}_{xy}$, as follows.

$$\boldsymbol{\rho}_{xy} = \sum_{i,j\in\{0,1\}^n} |A_i(x)\rangle|i_n\rangle|B_i(y)\rangle\langle A_j(x)|\langle j_n|\langle B_j(y)| = \boldsymbol{\rho}^0_{xy} + \boldsymbol{\rho}^1_{xy} + \widetilde{\boldsymbol{\rho}}_{xy},$$

where

$$\begin{aligned}
\boldsymbol{\rho}^0_{xy} &= \sum_{i,j\in\{0,1\}^n \text{ and } i_n=j_n=0} |A_i(x)\rangle|0\rangle|B_i(y)\rangle\langle A_j(x)|\langle 0|\langle B_j(y)|,\\
\boldsymbol{\rho}^1_{xy} &= \sum_{i,j\in\{0,1\}^n \text{ and } i_n=j_n=1} |A_i(x)\rangle|1\rangle|B_i(y)\rangle\langle A_j(x)|\langle 1|\langle B_j(y)|,
\end{aligned}$$

and $\widetilde{\boldsymbol{\rho}}_{xy} = \boldsymbol{\rho}_{xy} - \boldsymbol{\rho}^0_{xy} - \boldsymbol{\rho}^1_{xy}$ such that $\mathrm{Tr}(\boldsymbol{\rho}_{xy}) = \mathrm{Tr}(\boldsymbol{\rho}^0_{xy}) + \mathrm{Tr}(\boldsymbol{\rho}^1_{xy}) = 1$. Note that $\mathrm{Tr}(\boldsymbol{\rho}^0_{xy})$ (resp. $\mathrm{Tr}(\boldsymbol{\rho}^1_{xy})$) is the probability that the output of P is 0 (resp. 1). By basic properties of the trace [25], $\mathrm{Tr}(\boldsymbol{\rho}^0_{xy})$ can be written as follows: $|m_A\rangle$ and $|m_B\rangle$ are the computational base of Alice's and Bob's spaces, respectively, and $b \in \{0,1\}$. Then,

$$\begin{aligned}
\mathrm{Tr}(\boldsymbol{\rho}^0_{xy}) &= \sum_{m_A,b,m_B} \langle m_A|\langle b|\langle m_B|\boldsymbol{\rho}^0_{xy}|m_A\rangle|b\rangle|m_B\rangle\\
&= \sum_{m_A,m_B} \sum_{i,j\in\{0,1\}^{n-1}} \langle m_A|\langle m_B|(|A_{i0}(x)\rangle|B_{i0}(y)\rangle\langle A_{j0}(x)|\langle B_{j0}(y)|)|m_A\rangle|m_B\rangle\\
&= \sum_{i,j\in\{0,1\}^{n-1}} \sum_{m_A,m_B} \langle A_{j0}(x)|\langle B_{j0}(y)||m_A\rangle|m_B\rangle\langle m_A|\langle m_B||A_{i0}(x)\rangle|B_{i0}(y)\rangle\\
&= \sum_{i,j\in\{0,1\}^{n-1}} \langle A_{j0}(x)|A_{i0}(x)\rangle\langle B_{j0}(y)|B_{i0}(y)\rangle,
\end{aligned}$$

where the last equation holds since $\sum_{m_A,m_B} |m_A\rangle|m_B\rangle\langle m_A|\langle m_B| = I$ (completeness relation). Now, let us define the following vectors $\mathbf{a}(x) \in \mathbb{C}^{2^{2n-2}}$ and $\mathbf{b}(y) \in \mathbb{C}^{2^{2n-2}+1}$.

$$\begin{aligned}
(\mathbf{a}(x))_k = (\mathbf{a}(x))_{ij} &= \langle A_{j0}(x)|A_{i0}(x)\rangle,\\
(\mathbf{b}(y))_k = (\mathbf{b}(y))_{ij} &= \langle B_{j0}(y)|B_{i0}(y)\rangle \text{ for } i,j \in \{0,1\}^{n-1}, \quad (\mathbf{b}(y))_{2^{2n-2}+1} = 1/2,
\end{aligned}$$

where the index $k \in [2^{2n-2}]$ naturally corresponds to the index $ij \in \{0,1\}^{2n-2}$. Since P computes $f(x,y)$ with success probability $1/2+\epsilon$, $\mathrm{Tr}(\boldsymbol{\rho}^0_{xy}) \geq 1/2+\epsilon$ if $f(x,y) = 0$ and $\leq 1/2-\epsilon$ if $f(x,y) = 1$. Thus, the points $\mathbf{a}(x)$ and hyperplanes $\mathbf{b}(y)$ can be considered as an arrangement that "realizes" f but they are in complex space. Fortunately, one can find an arrangement in $\mathbb{R}^{2^{2n-1}}$ that realizes f from the above arrangement by noticing that $\mathrm{Tr}(\boldsymbol{\rho}^0_{xy})$ is always real. Namely,

$$\begin{aligned}
\mathrm{Tr}(\boldsymbol{\rho}^0_{xy}) &= \sum_{i,j\in\{0,1\}^{n-1}} \langle A_{j0}(x)|A_{i0}(x)\rangle\langle B_{j0}(y)|B_{i0}(y)\rangle = \sum_{k\in[2^{2n-2}]} (\mathbf{a}(x))_k(\mathbf{b}(y))_k\\
&= \sum_{k\in[2^{2n-2}]} \mathrm{Re}\left((\mathbf{a}(x))_k(\mathbf{b}(y))_k\right)\\
&= \sum_{k\in[2^{2n-2}]} (\mathrm{Re}(\mathbf{a}(x))_k\mathrm{Re}(\mathbf{b}(y))_k - \mathrm{Im}(\mathbf{a}(x))_k\mathrm{Im}(\mathbf{b}(y))_k)\\
&= \sum_{k\in[2^{2n-1}]} (\mathbf{a}'(x))_k(\mathbf{b}'(y))_k, \qquad (1)
\end{aligned}$$

where

$$(\mathbf{a}'(x))_{2k-1} = \mathrm{Re}(\mathbf{a}(x))_k, \quad (\mathbf{a}'(x))_{2k} = -\mathrm{Im}(\mathbf{a}(x))_k,$$
$$(\mathbf{b}'(y))_{2k-1} = \mathrm{Re}(\mathbf{b}(x))_k, \quad (\mathbf{b}'(y))_{2k} = \mathrm{Im}(\mathbf{b}(x))_k, \text{ for } k \in [2^{2n-2}],$$

and we set $(\mathbf{b}'(y))_{2^{2n-1}+1} = 1/2$. Now by Eq.(1), the arrangement of points $\mathbf{a}'(x)$ and hyperplanes $\mathbf{b}'(y)$ realizes f with margin ϵ. Also, it is easy to see that its magnitude is at most 1. Furthermore, since $\langle A_{i0}(x)|A_{i0}(x)\rangle$ and $\langle B_{j0}(y)|B_{j0}(y)\rangle$ are already real, the dimension of the above arrangement can be reduced from 2^{2n-1} to $2^{2n-1} - 2^{n-1}$. □

Proof of Theorem 3.2. Let $n = Q(f)$. As mentioned before Lemma 3.1, there exists an $(n+1)$-qubit shared-output protocol that computes f with success probability larger than $1/2$. By Lemma 3.3, we can obtain a $(2^{2n+1} - 2^n)$-dimensional arrangement realizing f. Thus $k_f \leq 2(2^n)^2 - 2^n$. By solving the quadratic inequality on 2^n, $Q(f) = n \geq \lceil \log(\sqrt{8k_f + 1} + 1) \rceil - 2$. The righthand side equals to $\lceil \log \sqrt{8k_f + 1} \rceil - 2 = \lceil \log \sqrt{k_f + 1/8} - 1/2 \rceil$ by a simple consideration on rounding reals, and hence we obtain the desired lower bound of $Q(f)$. On the contrary, it was proven that $Q^1(f) = \lceil \log \sqrt{k_f + 1} \rceil$ [14]. Since $Q(f) \leq \min(Q^1(f), Q^1(f^t))$ (by our definition mentioned before Lemma 3.1), we obtain the desired upper bound. These complete the proof.

4 Simultaneous Message Passing Models

The simultaneous message passing (SMP) model is the following three-party communication model: Alice and Bob have their inputs x and y, respectively, but they have no interaction at all. The third party with no access to input, called the *referee*, must compute a Boolean function $f(x, y)$ with the help of two messages sent from Alice and Bob. For such a model, the corresponding CC are defined similarly to two-way or one-way CCs.

We give quite tight characterizations of unbounded-error SMP CCs, $Q^{||}(f)$ and $C^{||}(f)$. First, we show the characterization of $Q^{||}(f)$ via k_f, which also implies that $Q^{||}(f)$ is the same as the sum of $Q^1(f)$ and $Q^1(f^t)$ up to two qubits.

Theorem 4.1 *For any Boolean function f, $Q^1(f) + Q^1(f^t) \leq Q^{||}(f) \leq Q^1(f) + Q^1(f^t) + 2$. In particular,*

$$\lceil \log \sqrt{k_f + 1} \rceil + \lceil \log \sqrt{k_{f^t} + 1} \rceil \leq Q^{||}(f) \leq 2\lceil \log \sqrt{k_f^* + 2} \rceil.$$

Proof. For lower bound, $Q^1(f) + Q^1(f^t) \leq Q^{||}(f)$ is obtained by considering the relation between one-way communication models and SMP models: In the SMP model, Alice must send at least $Q^1(f)$ qubits to the referee. Otherwise, the number of qubits that she sends to the referee would be $m < Q^1(f)$, and then we can construct an m-qubit one-way protocol from Alice to Bob by regarding the referee and Bob as the same party, which contradicts the definition of $Q^1(f)$. Similarly Bob must send at least $Q^1(f^t)$ qubits. Since $Q^1(f) = \lceil \log \sqrt{k_f + 1} \rceil$ for any f, we obtain $\lceil \log \sqrt{k_f + 1} \rceil + \lceil \log \sqrt{k_{f^t} + 1} \rceil \leq Q^{||}(f)$, and $2\lceil \log \sqrt{k_f^* + 2} \rceil \leq Q^1(f) + Q^1(f^t) + 2$.

What remains to do is to show the upper bound $Q^{||}(f) \leq 2\lceil \log \sqrt{k_f^* + 2} \rceil$. For this purpose, we can use *quantum fingerprinting* introduced in [5]. That is, Alice's input x and Bob's y are encoded into two quantum states $\boldsymbol{\rho}_x$ and $\boldsymbol{\rho}_y$, respectively, and the referee uses the controlled SWAP (C-SWAP) test. The difference from the standard quantum fingerprinting such as [5, 31, 13] is that

we use mixed states for encoding. (The C-SWAP test for mixed states are also used in [18] for quantum Merlin-Arthur games.)

We assume $k_f \leq k_{f^t}$ and show $Q^{||}(f) \leq 2\lceil \log \sqrt{k_f+2} \rceil$. (The case of $k_f > k_{f^t}$ is similarly shown.) Let $d = k_f$. Then there is an arrangement of points $\boldsymbol{p}_x = (p_i^x) \in \mathbb{R}^d$ and hyperplanes $\boldsymbol{h}_y = (h_i^y) \in \mathbb{R}^{d+1}$ that realizes f. Let $n = \lceil \log \sqrt{d+2} \rceil$ and $N = 2^n$. Also, for each x, define $\boldsymbol{q}_x = (q_i^x) \in \mathbb{R}^{d+1}$ as $q_1^x = p_1^x, \ldots, q_d^x = p_d^x$, $q_{d+1}^x = -1$. By Lemma 2.3, for each $\boldsymbol{q}_x$ and $\boldsymbol{h}_y$ we can obtain n-qubit states $\boldsymbol{\rho}(\boldsymbol{q}_x) = \frac{1}{N}\left(\boldsymbol{I} + \sqrt{\frac{N(N-1)}{2}} \sum_{i=1}^{d+1} \left(\frac{q_i^x}{|\boldsymbol{q}_x|(N-1)}\right) \boldsymbol{\lambda}_i\right)$ and $\boldsymbol{\rho}(\boldsymbol{h}_y) = \frac{1}{N}\left(\boldsymbol{I} + \sqrt{\frac{N(N-1)}{2}} \sum_{i=1}^{d+1} \left(\frac{h_i^y}{|\boldsymbol{h}_y|(N-1)}\right) \boldsymbol{\lambda}_i\right)$. Then, we consider the following SMP quantum protocol: (1) Alice and Bob send the referee $\boldsymbol{\rho}(\boldsymbol{q}_x)$ and $\boldsymbol{\rho}(\boldsymbol{h}_y)$, respectively. (2) The referee outputs the bit obtained by the C-SWAP test on the pair of the quantum states $(\boldsymbol{\rho}(\boldsymbol{q}_x), \boldsymbol{\rho}(\boldsymbol{h}_y))$ with probability $\alpha = \frac{1}{2}\left(\frac{1}{2} + \frac{1}{2N}\right)^{-1}$, and otherwise outputs 1 with probability $1-\alpha$. Note that the C-SWAP test produces output 0 with probability $\frac{1}{2} + \frac{1}{2}\mathrm{Tr}(\boldsymbol{\rho}(\boldsymbol{q}_x)\boldsymbol{\rho}(\boldsymbol{h}_y))$ [5, 18]. Thus, the referee outputs 0 with probability

$$\begin{aligned}
\alpha\left(\frac{1}{2} + \frac{1}{2}\mathrm{Tr}(\boldsymbol{\rho}(\boldsymbol{q}_x)\boldsymbol{\rho}(\boldsymbol{h}_y))\right) &= \frac{1}{2}\left(\frac{1}{2}+\frac{1}{2N}\right)^{-1}\left(\frac{1}{2} + \frac{1}{2N} + \frac{N-1}{2N}\sum_{i=1}^{d+1}\frac{q_i^x h_i^y}{|\boldsymbol{q}_x||\boldsymbol{h}_y|(N-1)^2}\right) \\
&= \frac{1}{2} + \frac{1}{4N|\boldsymbol{q}_x||\boldsymbol{h}_y|(N-1)}\left(\frac{1}{2}+\frac{1}{2N}\right)^{-1}\left(\sum_{i=1}^{d} p_i^x h_i^y - h_{d+1}^y\right) \\
&= \begin{cases} > 1/2 \text{ if } f(x,y) = 0 \\ < 1/2 \text{ if } f(x,y) = 1. \end{cases}
\end{aligned}$$

Hence $Q^{||}(f) \leq 2n = 2\lceil \log \sqrt{d+2} \rceil$. □

Moreover, we can also show a similar result in the classical setting.

Theorem 4.2 *For any Boolean function f, $C^1(f) + C^1(f^t) \leq C^{||}(f) \leq C^1(f) + C^1(f^t) + 1$. In particular,*

$$\lceil \log(k_f+1) \rceil + \lceil \log(k_{f^t}+1) \rceil \leq C^{||}(f) \leq \lceil \log(k_f^*+1) \rceil + \lceil \log(k_f^*+2) \rceil.$$

5 Weakly Unbounded-Error Communication Complexity

Finally we give several relations among the weakly unbounded-error CCs. For this purpose, we need Lemmas 2.1, 3.3 and 5.2 to consider the bias of the success probability explicitly when converting protocols to arrangement, and vice versa.

Theorem 5.1 *The following relations hold for any Boolean function f: (1) $C_w(f) \leq C_w^1(f) \leq 3Q_w(f) + O(1)$. (2) $Q_w^1(f) \leq 2Q_w(f) + O(1)$.*

Proof. 1) By the definition of $Q_w(f)$, there is a quantum protocol P such that $Q_w(f) = C_P + \lceil \log 1/\epsilon_P \rceil$ where C_P and $1/2 + \epsilon_P$ are the communication cost and the success probability of P, respectively. By Lemma 3.3, we can obtain a $(2^{2C_P-1} - 2^{C_P-1})$-dimensional arrangement of magnitude at most 1 with margin ϵ_P from P. By Lemma 2.1, we have a $2C_P$-bit one-way protocol that computes f with probability $\geq 1/2 + \epsilon_P/(2\sqrt{2^{2C_P-1}})$. This implies that $C_w^1(f) \leq 2C_P + \lceil \log(2\sqrt{2^{2C_P-1}}/\epsilon_P) \rceil$, which is at most $3C_P + \lceil \log 1/\epsilon_P \rceil + O(1) \leq 3Q_w(f) + O(1)$.

2) The proof idea is similar to 1). The difference from 1) is to construct a desired protocol from the arrangement. To this end, we use the following lemma, whose proof is omitted, that convert

arrangements to one-way quantum CC. The proof follows from carefully transforming points and hyperplanes, with appropriate shrinking and shifting factors, to quantum states (by Lemma 2.3) and measurements (by Lemma 2.4), respectively. The success probabilities of resulting protocols then follows from Lemma 5 of [14].

Lemma 5.2 (From arrangements to quantum CC) *Each d-dimensional arrangement of magnitude at most 1 realizing f with margin μ can be converted into an $n = \lceil \log \sqrt{d+1} \rceil$ qubit one-way protocol that computes f with success probability at least $1/2 + \alpha\mu$ where $\alpha = \frac{\sqrt{2}-1}{2^{n+1/2}}$.*

Now we give the proof of Theorem 5.1 (2). Take a quantum protocol P such that $Q_w(f) = C_P + \lceil \log 1/\epsilon_P \rceil$ where C_P and $1/2 + \epsilon_P$ are the communication cost and the success probability of P, respectively. By Lemma 3.3, we can obtain a $(2^{2C_P-1} - 2^{C_P-1})$-dimensional arrangement of magnitude at most 1 with margin ϵ_P from P. By Lemma 5.2, we have a one-way quantum protocol for f using at most C_P qubits such that its success probability is $1/2 + \Omega(\epsilon_P/2^{C_P})$. This implies that $Q^1_w(f) \leq 2C_P + \lceil \log 1/\epsilon_P \rceil + O(1) \leq 2Q_w(f) + O(1)$. □

Similar to the proof of Theorem 5.1, using the proofs of Theorems 4.1 and 4.2 we can also show: $Q^{||}_w(f) \leq 4Q_w(f) + O(1)$ and $C^{||}_w(f) \leq 9Q_w(f) + O(1)$.

Acknowledgements

We would like to acknowledge Francois Le Gall for insightful discussion on the two-way model, and Prof. Hiroshi Imai of University of Tokyo and ERATO-SORST project for partial support that enabled us to have a useful face-to-face discussion with quantum computation and information researchers in Japan while writing the paper.

References

[1] N. Alon, P. Frankl and V. Rödl. Geometrical realization of set systems and probabilistic communication complexity. *Proc. 26th FOCS*, pp. 277–280, 1985.

[2] A. Ambainis, A. Nayak, A. Ta-shma and U. Vazirani. Dense quantum coding and quantum finite automata. *J. ACM* **49** (2002) 496–511.

[3] L. Babai, P. Frankl and J. Simon. Complexity classes in communication complexity. *Proc. 27th FOCS*, pp. 303–312, 1986.

[4] L. Babai and P. Kimmel. Randomized simultaneous messages: solution of a problem of Yao in communication complexity. *Proc. 12th CCC*, pp. 239–246, 1997.

[5] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.* **87** (2001) Article no. 167902.

[6] H. Buhrman, N. Vereshchagin and R. de Wolf. On computation and communication with small bias. *Proc. 22nd CCC*, pp. 24–32, 2007.

[7] H. Buhrman and R. de Wolf. Communication Complexity Lower Bounds by Polynomials. *Proc. 16th CCC*, pp. 120–130, 2001. Also, cs.CC/9910010.

[8] J. Forster. A linear lower bound on the unbounded error probabilistic communication complexity. *J. Comput. Syst. Sci.* **65** (2002) 612–625.

[9] J. Forster, M. Krause, S. V. Lokam, R. Mubarakzjanov, N. Schmitt and H. U. Simon. Relations between communication complexity, linear arrangements, and computational complexity. *Proc. 21th FSTTCS, Lecture Notes in Comput. Sci.* **2245** (2001) 171–182.

[10] J. Forster and H. U. Simon. On the smallest possible dimension and the largest possible margin of linear arrangements representing given concept classes. *Theoret. Comput. Sci.* **350** (2006) 40–48.

[11] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz and R. de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. *Proc. 39th STOC*, pp. 516–525, 2007. Also, quant-ph/0611209.

[12] D. Gavinsky, J. Kempe, O. Regev and R. de Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. *Proc. 38th STOC*, pp. 594–603, 2006.

[13] D. Gavinsky, J. Kempe and R. de Wolf. Strengths and weaknesses of quantum fingerprinting. *Proc. 21st CCC*, pp. 288–298, 2006.

[14] K. Iwama, H. Nishimura, R. Raymond and S. Yamashita. Unbounded-error one-way classical and quantum communication complexity. *Proc. 34th ICALP, Lecture Notes in Comput. Sci.* **4596** (2007) 110–121. Also, quant-ph/0706.3265.

[15] L. Jakóbczyk and M. Siennicki. Geometry of Bloch vectors in two-qubit system. *Phys. Lett. A* **286** (2001) 383–390.

[16] G. Kimura and A. Kossakowski. The Bloch-vector space for N-level systems – the spherical-coordinate point of view. *Open Sys. Information Dyn.* **12** (2005) 207–229.

[17] H. Klauck. Lower bounds for quantum communication complexity. *SIAM J. Comput.* **37** (2007) 20–46.

[18] H. Kobayashi, K. Matsumoto and T. Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? *Proc. 14th ISAAC, Lecture Notes in Comput. Sci.* **2906** (2003) 189–198.

[19] A. Kossakowski. A class of linear positive maps in matrix algebras. *Open Sys. Information Dyn.* **10** (2003) 213–220.

[20] I. Kremer. *Quantum Communication*. Master's Thesis, The Hebrew Univ. of Jerusalem, 1995.

[21] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge, 1997.

[22] N. Linial and A. Shraibman. Learning complexity vs. communication complexity. Manuscript, 2006. Available at http://www.cs.huji.ac.il/~nati/

[23] N. Linial and A. Shraibman. Lower bounds in communication complexity based on factorization norms. *Proc. 39th STOC*, pp. 699–708, 2007.

[24] I. Newman and M. Szegedy. Public vs. private coin flips in one-round communication games. *Proc. 28th STOC*, pp. 561–570, 1996.

[25] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge, 2000.

[26] R. Paturi and J. Simon. Probabilistic communication complexity. *J. Comput. Syst. Sci.* **33** (1986) 106–123. Preliminary version appeared in *Proc. 25th FOCS*, pp. 118–126, 1984.

[27] R. Raz. Exponential separation of quantum and classical communication complexity. *Proc. 31st STOC*, pp. 358–367, 1999.

[28] A. Sherstov. Halfspace matrices. *Proc. 22nd CCC*, pp. 83–95, 2007.

[29] R. de Wolf. Nondeterministic quantum query and communication complexities. *SIAM J. Comput* **32** (2003) 681–699.

[30] A. C.-C. Yao. Quantum circuit complexity. *Proc. 34th FOCS*, pp. 352–360, 1993.

[31] A. C.-C. Yao. On the power of quantum fingerprinting. *Proc. 35th STOC*, pp. 77–81, 2003.